DIALOG(R)File 345:Inpadoc/Fam.& Legal Stat

18123608
Basic Patent (No,Kind,Date): JP 2002258975 A2 20020913 <No. of Patents: 001>
DEVICE FOR IDENTIFYING FINGERPRINT AND METHOD FOR THE SAME (English)
Patent Assignee: NIPPON TELEGRAPH & TELEPHONE
Author (Inventor): ARAME TETSUO; AKISHINO KEIZO; OKI NOBUHIRO
IPC: *G06F-001/00; G06F-015/00; H04L-009/32
Language of Document: Japanese
Patent Family:

Patent No	Kind	Date	Applic No	Kind	Date	
JP 2002258975	A2	20020913	JP 200152468	A	20010227	(BASIC)

Priority Data (No,Kind,Date):
JP 200152468 A 20010227

DIALOG(R)File 347:JAPIO

07390474 **Image available**
DEVICE FOR IDENTIFYING FINGERPRINT AND METHOD FOR THE SAME

PUB. NO.: 2002-258975 [JP 2002258975 A]
PUBLISHED: September 13, 2002 (20020913)
INVENTOR(s): ARAME TETSUO
AKISHINO KEIZO
OKI NOBUHIRO
APPLICANT(s): NIPPON TELEGRAPH & TELEPHONE EAST CORP
APPL. NO.: 2001-052468 [JP 200152468]
FILED: February 27, 2001 (20010227)
INTL CLASS: G06F-001/00; G06F-015/00; H04L-009/32

ABSTRACT

PROBLEM TO BE SOLVED: To provide a fingerprint identifying device capable of strengthening the identification (confirmation) of a person himself or herself, and preventing any danger for infringement of his or her privacy.

SOLUTION: A user inserts an IC card 14 in which the fingerprint data of the user himself or herself and a log-on ID are preliminarily stored into a reading/identifying device 15, and allows the device 15 to read the

fingerprint picture of the user himself or herself from a fingerprint reading screen 15a of the device 15. The device 15 collates the fingerprint picture of the user with the fingerprint data of the user stored in the IC card 14, and when they coincide with each other, the device 15 reads the log-on ID from the IC card 14. A task terminal 11 receives the result of the fingerprint identification and the log-on ID (when the identification is successful) from the device 15, and when the received log-on ID coincides with a log-on ID stored in a storage device 13, the task terminal 11 permits the user to use the task terminal.

(19)日本国特許庁（ＪＰ）　(12)公開特許公報（A）　(11)特許出願公開番号
特開2002－258975
（P2002－258975A）
(43)公開日　平成14年９月13日(2002.9.13)

(51)Int.Cl.'		識別記号	FI		テーマコード'(参考)
G06F	1/00	370	G06F	1/00	370E　5B085
	15/00	330		15/00	330F　5J104
					330G
H04L	9/32		H04L	9/00	673E
					673D

審査請求　未請求　請求項の数３　ＯＬ　（全５頁）

(21)出願番号　特願2001－52468(P2001－52468)

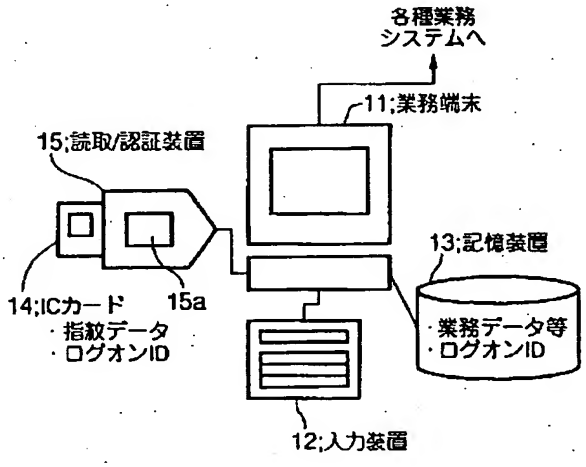
(22)出願日　平成13年２月27日(2001.2.27)

(71)出願人　399040405
東日本電信電話株式会社
東京都新宿区西新宿三丁目19番２号
(72)発明者　新目　徹夫
東京都新宿区西新宿三丁目19番２号　東日本電信電話株式会社内
(72)発明者　秋篠　敬三
東京都新宿区西新宿三丁目19番２号　東日本電信電話株式会社内
(74)代理人　100064908
弁理士　志賀　正武

最終頁に続く

(54)【発明の名称】　指紋認証装置および指紋認証方法

(57)【要約】
【課題】　従来以上に本人の認証（確認）を強化することができ、しかも、プライバシーの侵害の虞れがない指紋認証装置を提供する。
【解決手段】　ユーザは、自身の指紋データとログオンＩＤが予め記憶されたＩＣカード１４を読取／認証装置１５に挿入し、そして、読取／認証装置１５の指紋読取面１５ａから自身の指紋画像を読み込ませる。読取／認証装置１５は、ユーザの指紋画像と、ＩＣカード１４に記憶されたユーザの指紋データとを照合し、一致した場合はＩＣカード１４からログオンＩＤを読み出す。業務端末１１は、読取／認証装置１５から指紋認証の結果と、認証が成功した場合はログオンＩＤとを受け取り、受け取ったログオンＩＤが記憶装置１３内に記憶されているのログオンＩＤと一致した場合に、ユーザに対して業務端末の利用を許可する。



【特許請求の範囲】
【請求項１】　ユーザの指紋データおよび識別番号が記憶されたカードと、
前記ユーザの識別番号が記憶された記憶手段と、
前記ユーザの指紋を読み取る指紋読取手段と、
前記カードの指紋データおよび識別番号を読み取る読取手段と、
前記カードから読み取られた指紋データと前記指紋読取装置によって読み取られたユーザの指紋とを比較し、両者が一致しているか否かを判定する第１の認証手段と、
前記カードから読み取られた識別番号と前記記憶手段内の識別番号とを比較し、両者が一致しているか否かを判定する第２の認証手段と、
を具備し、前記第１、第２の認証手段による認証結果が共に「一致している」であった場合に認証結果が良であると判定することを特徴とする指紋認証装置。
【請求項２】　前記記憶手段および前記第２の認証装置を前記第１の認証装置に対し遠隔地に設け、両者間を通信回線で接続したことを特徴とする請求項１に記載の指紋認証装置。
【請求項３】　ユーザの指紋を取得する第１の処理と、
ユーザのカードから指紋データを取得する第２の処理と、
ユーザの指紋と前記指紋データとを比較し、両者が一致しているか否かを判定する第３の処理と、
前記第３の処理の判定結果が一致であった場合に、前記カードから識別番号を読み取る第４の処理と、
該識別番号と記憶手段内に予め記憶されている識別番号とを比較し、両者が一致しているか否かを判定する第５の処理と、
前記第５の処理による判定結果が「一致」であった場合に、認証結果が良であると判定することを特徴とする指紋認証方法。
【発明の詳細な説明】
【０００１】
【発明の属する技術分野】この発明は、システムログオン時にユーザ認証を行う認証装置に係り、特に、ＩＣカードに記憶された電子データの読取りと、指紋読取りとに基づいて認証を行う指紋認証装置および指紋認証方法に関する。
【０００２】
【従来の技術】従来、システムログオン時にユーザ認証を行う方法として、①ユーザが暗証番号やパスワードを入力する、②ユーザがカード読み取り器にカードを挿入し、読み取り器がカード上に取り付けられた媒体の磁気／電子データを読み取ってデータベースと照合することで本人確認を行う、③ユーザの指紋を照合する等の方法が知られている。
【０００３】図３は、従来のユーザ認証方法を説明するためのシステム構成例を示す図であり、ユーザは業務端末１を利用する際に、入力装置（キーボード）２から暗証番号／パスワードを入力する。業務端末１は入力装置２からの入力されたデータと、予め記憶装置３に記憶されている認証データとを照合し、一致した場合に、ユーザに対して業務端末１の利用を許可する。この場合、正規のユーザに与えられる暗証番号／パスワードが不正に第三者に知られた場合、業務端末１を不正利用される恐れがある。
【０００４】これに対し、指紋認証による場合、ユーザは業務端末１を利用する際に、指紋読取装置４によって指紋画像を読み込ませる。業務端末１は指紋読取装置４によって読取った指紋画像と、記憶装置３に記憶されている指紋データとを照合し、一致した場合に、ユーザに対して業務端末１の利用を許可する。この場合、記憶装置３の指紋データが不正に第三者に漏洩した場合、プライバシーの侵害になるため、ユーザが記憶装置３への指紋データの登録に抵抗を示すことがある。また、利用する業務端末全てにユーザの指紋データを登録する必要があり、運用が複雑になる欠点がある。
【０００５】図４は、従来のユーザ認証を説明するための他のシステム構成例を示す図である。ユーザは、業務端末５を使用する際に、指紋読取装置６からから指紋画像を読み込ませる。業務端末５は指紋読取装置６によって読取った指紋画像を、通信回線７を経由して業務サーバ８へ送信する。業務サーバ８は、その指紋画像と記憶装置９に格納された指紋データとを照合し、照合結果を通信回線７を介して業務端末５へに返送する。業務端末５は業務サーバ８からの結果を受けて、指紋認証が成功した場合にはユーザに業務端末５の利用を許可する。この方法の場合、ユーザが別の業務端末を使用する場合に、指紋データを再登録する必要はないが、記憶装置９の指紋データが流出した場合、多数のユーザに対してプライバシーの侵害が発生する問題がある。
【０００６】
【発明が解決しようとする課題】上述したように、暗証番号やパスワードあるいはカードによる認証の場合、盗難により本人以外の者が不正に業務システムを利用してしまう虞れがあり、一方、指紋による認証の場合、指紋データが流出した時にプライバシーが侵害される虞れがあることから、ユーザにとって事前の指紋登録に対して心理的な抵抗があるという欠点がある。
【０００７】この発明は、このような事情を考慮してなされたもので、その目的は、従来以上に本人の認証（確認）を強化することができ、しかも、プライバシーの侵害の虞れがない指紋認証装置および指紋認証方法を提供することにある。
【０００８】
【課題を解決するための手段】この発明は上記の課題を解決すべくなされたもので、請求項１に記載の発明は、ユーザの指紋データおよび識別番号が記憶されたカード

と、前記ユーザの識別番号が記憶された記憶手段と、前記ユーザの指紋を読み取る指紋読取手段と、前記カードの指紋データおよび識別番号を読み取る読取手段と、前記カードから読み取られた指紋データと前記指紋読取装置によって読み取られたユーザの指紋とを比較し、両者が一致しているか否かを判定する第１の認証手段と、前記カードから読み取られた識別番号と前記記憶手段内の識別番号とを比較し、両者が一致しているか否かを判定する第２の認証手段とを具備し、前記第１、第２の認証手段による認証結果が共に「一致している」であった場合に認証結果が良であると判定することを特徴とする指紋認証装置である。

【０００９】また、請求項２に記載の発明は、請求項１に記載の指紋認証装置において、前記記憶手段および前記第２の認証装置を前記第１の認証装置に対し遠隔地に設け、両者間を通信回線で接続したことを特徴とする。また、請求項３に記載の発明は、ユーザの指紋を取得する第１の処理と、ユーザのカードから指紋データを取得する第２の処理と、ユーザの指紋と前記指紋データとを比較し、両者が一致しているか否かを判定する第３の処理と、前記第３の処理の判定結果が一致であった場合に、前記カードから識別番号を読み取る第４の処理と、該識別番号と記憶手段内に予め記憶されている識別番号とを比較し、両者が一致しているか否かを判定する第５の処理と、前記第５の処理による判定結果が「一致」であった場合に、認証結果が良であると判定することを特徴とする指紋認証方法である。

【００１０】

【発明の実施の形態】以下、図面を参照し、この発明の実施の形態について説明する。図１はこの発明の第１の実施の形態による指紋認証装置を適用したシステムの構成を示すブロック図であり、この図において、１１は業務端末、１２は入力装置、１３は記憶装置である。この記憶装置１３には、予め、業務端末１１を使用するユーザのログオンＩＤが記憶されている。１４はユーザが所有するＩＣカードであり、所有者のログオンＩＤおよび指紋データが記憶されている。１５はＩＣカード１４を読み取る読取装置、指紋を読み取る指紋読取装置および指紋照合を行う認証装置の機能を有する読取／認証装置である。

【００１１】このような構成において、ユーザは、業務端末１１を利用する際にユーザの指紋データとログオンＩＤが予め記憶されたＩＣカード１４を読取／認証装置１５に挿入し、そして、読取／認証装置１５の指紋読取面１５ａから指紋画像を読み込ませる。一方、業務端末１１は読取／認証装置１５に対して、指紋認証結果とログオンＩＤを要求する。読取／認証装置１５は、ユーザの指紋画像と、ＩＣカード１４に記憶されたユーザの指紋データとを照合し、一致した場合はＩＣカード１４からログオンＩＤを読出す。業務端末１１は、読取／認証装置１５から指紋認証の結果と、認証が成功した場合はログオンＩＤとを受け取り、受け取ったログオンＩＤが記憶装置１３内に記憶されているのログオンＩＤと一致した場合に、ユーザに対して業務端末の利用を許可する。

【００１２】上記実施形態によれば、ＩＣカード１４内の電子データのチェックと、指紋認証により、セキュリティの強化を図ることができる。また、指紋照合時に使用するユーザの指紋データは、個人が保持するしているので、プライバシーの保護を図ると共に、別の業務端末を利用する場合にも指紋データを再登録する必要がない利点がある。また、本実施形態は構成が単純であり、かつ、照合機能も備えていることから、既存の業務端末に組み込むことが容易である。

【００１３】次に、この発明の第２の実施形態について説明する。図２は同実施形態による指紋認証装置を適用したシステムの構成を示すブロック図であり、この図において、２１は業務端末である。２４はユーザが所有するＩＣカードであり、上記第１の実施形態と同様に、所有者のログオンＩＤおよび指紋データが記憶されている。２５は上述した読取／認証装置１５と同様に構成された読取／認証装置である。２６は通信回線、２７は業務サーバ、２８は業務サーバ２７によって書込／読出が行われる記憶装置である。この記憶装置２３には、予め、業務端末２１を使用するユーザのログオンＩＤが記憶されている。

【００１４】このような構成において、ユーザは業務端末２１を利用する際に、ユーザの指紋データとログオンＩＤを保持したＩＣカード２４を読取／認証装置２５に挿入し、指紋読取面２５ａからから自身の指紋画像を読み取らせる。業務端末２１は読取／認証装置２５に対して、指紋認証とログオンＩＤを要求する。読取／認証装置２５はユーザの指紋画像と、ＩＣカード２４に記憶されたユーザの指紋データとを照合し、一致した場合はＩＣカードからログオンＩＤを読出す。業務端末２１は、読取／認証装置２５から認証結果と、認証が成功した場合はログオンＩＤを受け取り、受け取ったログオンＩＤを通信回線２６を介して業務サーバ２７へ送信する。業務サーバ２７は受け取ったログオンＩＤと記憶装置２８内のログオンＩＤとを照合し、その結果を通信回線２６を介して業務端末２１に返送する。業務端末２１は照合結果が一致していた場合、ユーザに対して業務端末２１の利用を許可する。

【００１５】上述した第２の実施形態によれば、ユーザ個人が所有するＩＣカード内に指紋データを格納することから、カードの盗難があった場合でも、そのカード所有者以外の指紋データが流出する危険を回避することができる。また、本実施形態を用いると、既存の業務システムに別途指紋データ共用装置等を用意することなく、容易に指紋認証によるログオン方式を組み込むことが可

能となる利点がある。

【００１６】

【発明の効果】以上説明したように、この発明によれば、既存の暗証番号・パスワード入力方式や、カード上の媒体から磁気／電子データを読み取る方式に比較し、本人性確認が強化され、業務システムのユーザに対するセキュリティが向上する効果が得られる。また、業務システム端末や、業務システムのデータベース内に指紋データを保持すると、流出する危険性があるが、そのような危険を排除することができ、プライバシー保護を図ることができる。また、磁気カード読取り装置と指紋読取装置を一体化し、装置に指紋照合機能を持たせることで、装置の小型化を図ることが出来ると共に、演算能力の低い端末（一般のパーソナルコンピュータ等）への組込み用途としても最適であり、既存の業務システムのセキュリティ強化を図ることが出来る。

【図面の簡単な説明】

【図１】　この発明の第１の実施形態の構成を示すブロック図である。

【図２】　この発明の第２の実施形態の構成を示すブロック図である。

【図３】　従来のユーザ認証方法を説明するためのシステム構成例を示す図である。

【図４】　従来のユーザ認証方法を説明するための他のシステム構成例を示す図である。

【符号の説明】

１１，２１…業務端末

１３…記憶装置

１４、２４…ＩＣカード

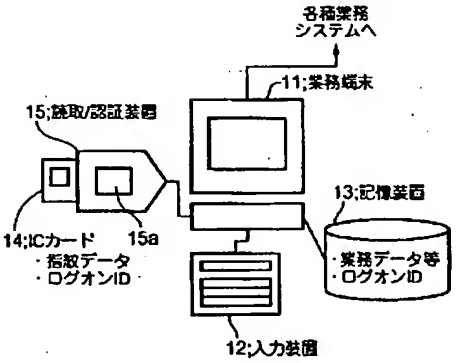
１５、２５…読取／認証装置

２６…通信回線

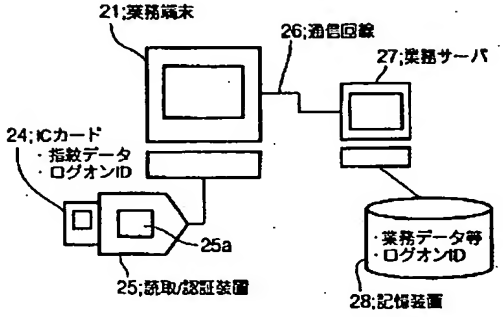
２７…業務サーバ

２８…記憶装置。

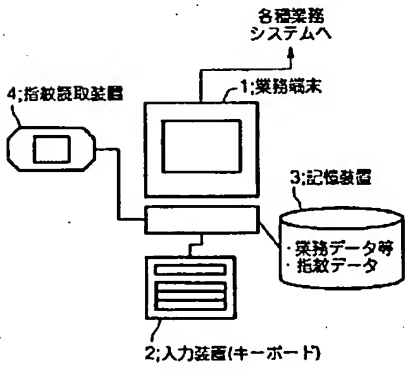
【図１】



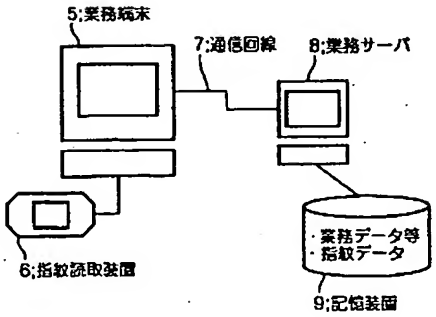
【図２】



【図３】



【図４】



フロントページの続き

(72)発明者 沖 宣宏
東京都新宿区西新宿三丁目19番２号 東日本電信電話株式会社内

Fターム(参考) 5B085 AE12 AE23 AE26 BC01
5J104 AA07 KA01 KA17 NA05 NA35
NA38 NA41 PA07